UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

THOMAS LUCA, on behalf of himself and all others similarly situated, Plaintiff, v. ONETOUCHPOINT, INC., Defendant.	Case No.: 2:22-cv-912 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Thomas Luca ("Plaintiff") brings this Class Action Complaint on behalf of himself, and all others similarly situated, against Defendant, OneTouchPoint, Inc. ("OTP" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge:

NATURE OF THE CASE

1. Business associates of healthcare providers that handle sensitive, personally identifying information ("PII") or protected health information ("PHI") owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII or PHI to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a data breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time

and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

3. OTP is a healthcare provider vendor who provides printing and mailing marketing services to various health insurance carriers and medical providers ("Customer-Healthcare Providers"). To provide these services, OPT knowingly obtains PII and PHI from healthcare providers which Defendant then utilizes to conduct mailings on behalf of its Customer-Healthcare Providers.

4. As the business associate of healthcare providers, OTP knowingly obtains patient PII and PHI from its Customer-Healthcare Providers and has a resulting duty to securely maintain such information in confidence.

5. OTP states that it "adhere[s] to the strictest HIPAA standards and ensure[s] that the handling of protected health information (PHI) is secure. OneTouchPoint will sign a Business Associates Agreement (BAA) with our customers to become joint custodians of protected health information (PHI)."[1]

6. Plaintiff brings this class action on behalf of individuals whose PII and PHI was provided to OTP by their healthcare providers and was accessed and/or exposed to unauthorized third parties during a data breach of OTP's system, which OTP states began on April 27, 2022, and involved "printing and mailing services" OTP provides for approximately 34 Customer-Healthcare Providers (the "Data Breach").

[1] OneTouchPoint, *Solutions/Healthcare*, https://1touchpoint.com/solutions/healthcare, (last visited Aug. 8, 2022).

7. Despite that OTP became aware of the Data Breach by April 28, 2022,[2] it failed to notify Plaintiff and the putative Class Members within sixty (60) days as required by law. Notably, OTP failed to notify Plaintiff of the Data Breach for three months from its discovery of the same.

8. Plaintiff on behalf of himself and the Class as defined herein, brings claims for negligence, negligence *per se*, breach of fiduciary duty, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

9. Based on the public statements of OTP to date, as well as statements by its Customer-Healthcare Providers, a wide variety of PII and PHI was implicated in the breach, including full names, addresses, healthcare member IDs, and information provided during health assessments (*i.e.*, diagnoses, medications, dates of birth, sexes, physical demographics information, family histories, social histories, allergies, vitals, and immunizations). [3]

10. As a direct and proximate result of OTP's inadequate data security, and its breach of its duty to handle PII and PHI with reasonable care, Plaintiff's and Class Members' PII and PHI has been accessed by hackers and exposed to an untold number of unauthorized individuals.

11. Plaintiff and Class Members are now at a significantly increased risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, which risk may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

---

[2] OneTouchPoint, *Notice of Data Security Event*, https://1touchpoint.com/notice-of-data-event, (last visited August 8, 2022).

[3] *Id.; see also* Jonathan Greig*, At Least 34 Healthcare Orgs Affected by Alleged Ransomware Attack on OneTouchPoint*, The Record (Aug. 1, 2022), https://therecord.media/at-least-34-healthcare-orgs-affected-by-alleged-ransomware-attack-on-onetouchpoint/.

12. To recover from OTP for these harms, Plaintiff and the Class seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring OTP to: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII and PHI possessed by OTP; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

13. Plaintiff Thomas Luca is an adult who at all relevant times has been a citizen and resident of the Commonwealth of Pennsylvania.

14. Defendant OneTouch Point, Inc. is a corporation organized under the laws of Wisconsin, with its principal place of business located at 1225 Walnut Ridge Dr., Hartland, Wisconsin 53029-8300.

JURISDICTION AND VENUE

15. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

16. This Court has personal jurisdiction over OTP because OTP has its principal place of business in Wisconsin.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) and (2), because this is the District in which OTP resides, and is where a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred.

FACTUAL BACKGROUND

A. OneTouchPoint and the Services Provided.

18. OTP provides online and offline traditional marketing and communication strategies to Customer-Healthcare Providers to help them find and engage patients.

19. OTP provides these services to Customer-Healthcare Providers nationwide.

20. Upon information and belief, while administering its marketing and communication services, OTP receives, maintains, and handles PII and PHI from its Customer-Healthcare Providers, which includes, *inter alia*, individuals' names, birthdates, addresses, healthcare member IDs, service dates, service descriptions, diagnosis codes, and health evaluation dates.

21. Upon information and belief, because OTP receives, maintains, and handles PII and PHI from its Customer-Healthcare Providers, OTP qualifies as a business associate within the meaning of 45 CFR § 160.103(3) and has therefore entered into Business Associate Agreements with its Customer-Healthcare Providers, becoming a custodian of PHI.

22. As a business associate of its Customer-Healthcare Providers, OTP is a covered entity under the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 1302d, *et seq*.

23. Plaintiff and Class Members directly or indirectly entrusted OTP with their sensitive and confidential PII and PHI and therefore reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

24. As a custodian of Plaintiff's and Class Members' PII and PHI, Defendant assumed equitable and legal duties to safeguard and keep confidential Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

B. OTP Knew the Risks of Storing Valuable PII and PHI and the Foreseeable Harm to Victims.

25. At all relevant times, OTP knew it was storing sensitive PII and PHI and that, as a result, OTP's systems would be attractive for cybercriminals.

26. OTP also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

27. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, Blackbaud, and many others.

28. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers can easily sell stolen data as well as the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[4] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

29. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[5]

---

[4] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited Aug. 8, 2022).

[5] *Data Breach Report: 2021 Year End*, Risk Based Security (February 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/ (last accessed Aug. 8, 2022).

30. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[6]

31. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[7]

32. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it quickly – making the industry a growing target."[8]

33. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves individuals, whose PII and PHI Defendant possesses, especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

34. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[9] A complete identity theft kit that includes health insurance credentials may be

---

[6] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Aug. 8, 2022).

[7] SwivelSecure, *The healthcare industry is at risk*, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited on Aug. 8, 2022).

[8] *Id.*

[9] IDExperts, You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows: https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited Aug. 8, 2022).

worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[10]

35. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[11]

36. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that

[10] PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world*, Key findings from The Global State of Information Security® Survey 2015: https://www.pwc.com /gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited Aug. 8, 2022).

[11] Experian, Healthcare Data Breach: What to Know About them and What to Do After One: https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited Aug. 8, 2022).

attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[12]

37. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

38. OTP certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

C. OTP Breached its Duty to Protect the PII and PHI in its Custody.

39. On or around July 27, 2022, Defendant released a "Notice of Data Security Event" ("Notice") that announced on or around April 28, 2022, OTP was alerted to unauthorized access to OTP servers and that it discovered encrypted files on certain computer systems.[13]

40. Shortly thereafter, Plaintiff received a "Notice of Data Event" dated July 27, 2022 ("Letter"), indicating that his PII and PHI may have been compromised by the Data Breach.

41. According to OTP, it investigated "the nature and scope of the activity," and it alleged that it has "no evidence of misuse of any information related to this incident" but also encouraged "individual to remain vigilant against incidents of identity theft and fraud, to review

[12] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Aug. 8, 2022).

[13] OneTouchPoint, *Notice of Data Security Event*, https://1touchpoint.com/notice-of-data-event, (last visited August 8, 2022).

account statements and explanation of benefits forms, and monitor[] free credit reports for suspicious activity, and detect errors."[14] Thus, based on the amount of sensitive information OTP possesses, it would be naïve to believe the cybercriminals did not purposefully steal sensitive information with a specific intent to use it or sell it to others who will.

42. OTP determined that the information impacted included: "an individual's name, [healthcare] member ID, and information that may have [been] provided during a health assessment."[15] However, OTP's Customer-Healthcare Providers have issued their own data breach notifications, informing individuals that their "ID numbers, diagnoses, medications, addresses, dates of birth, sexes, physician demographics information, family histories, social histories, allergies, vitals, immunizations, and more" were exposed as a result of the Data Breach.[16]

43. The unauthorized persons gained access to the PII and PHI of approximately 1 million patients of OTP's Customer-Healthcare Providers.[17]

44. While the Data Breach occurred in April, Defendant alerted the public and affected individuals at the end of July, three full months after the breach. In those months OTP left the public in the dark and it failed to inform individuals of the danger posed by the ongoing breach. Even now, OTP's disclosures have been vague and evasive, leaving Plaintiff and class members with incomplete information regarding the true nature and extent of the Data Breach.

---

[14] *Id.*

[15] *Id.*

[16] Jonathan Greig, *At Least 34 Healthcare Orgs Affected by Alleged Ransomware Attack on OneTouchPoint*, The Record (Aug. 1, 2022), https://therecord.media/at-least-34-healthcare-orgs-affected-by-alleged-ransomware-attack-on-onetouchpoint/.

[17] *Data Breach Notifications*, OFF. ME. ATT'Y GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/0a2e4b99-8e95-4860-b05f-62c239a13993.shtml, (last visited Aug. 8, 2022).

45. The Data Breach occurred as a direct result of OTP's failure to implement and follow basic security procedures in order to protect its patients' PII and PHI.

46. OTP says it "take[s] "the confidentiality, privacy, and security of information in its care seriously" yet sent alerts to individuals affected of the Data Breach after it was too late for individuals to safeguard their information and provides no assistance to individuals affected by the Data Breach in the event of their identity being stolen.[18]

D. Plaintiff and Class Members Suffered Damages.

47. For the reasons mentioned above, OTP's conduct, which allowed the Data Breach to occur, caused the Plaintiff and members of the Class significant injuries and harm in several ways. Plaintiff and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

48. Once PII and PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or protected against future misuse. For this reason, Plaintiff and Class members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of OTP's conduct. Further, the value of Plaintiff's and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

[18] OneTouchPoint, *Notice of Data Security Event*, https://1touchpoint.com/notice-of-data-event, (last visited Aug. 8, 2022).

49. As a result of OTP's failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PHI.

50. Plaintiff and Class Members are also at a continued risk because their information remains in OTP's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as OTP fails to undertake the necessary and appropriate security and training measures to protect the PII and PHI of its Customer-Healthcare Providers' patients in its possession.

51. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

CLASS ALLEGATIONS

52. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following class:

> All individuals in the United States whose PII and/or PHI was compromised in the OneTouchPoint, Inc. data breach disclosed by Defendant on July 27, 2022 (the "Class").

53. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

54. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when he moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

55. The requirements of Rule 23(a)(1) are satisfied. The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective class members through this class action will benefit both the parties and this Court. The exact size of the class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach, but based on public information, the Class includes approximately 1 million individuals.

56. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest, and there are common questions of fact and law affecting members of the Class. The questions of fact and law common to the Class predominate over questions which may affect individual members and include the following:

a. Whether Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached its duties thereby;

c. Whether Defendant breached its fiduciary duty to Plaintiff and the Class;

d. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

e. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

57. The requirements of Rule 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same failure by Defendant to safeguard PII and PHI.

58. OTP was the custodian of Plaintiff's and Class Members' PII and PHI, when their PII and PHI was obtained by an unauthorized third party.

59. The requirements of Rule 23(a)(4) are satisfied. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class members are substantially identical as explained above.

60. The requirements of Rule 23(b)(3) are satisfied here because a class action is the superior method of litigation for these issues, and common issues will predominate. While the aggregate damages that may be awarded to the members of the Class are likely to be substantial, the damages suffered by the individual members of the Class are relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a Class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation method available to Plaintiff and the Class and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Class. Defendant's uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class member.

FIRST CAUSE OF ACTION
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE CLASS)

61. Plaintiff restates and realleges all proceeding factual allegations above as if fully set forth herein.

62. OTP owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

63. OTP's duty to use reasonable care arose from several sources, including but not limited to those described below.

64. OTP had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By receiving, maintaining, and handling PII and PHI that is routinely targeted by criminals for unauthorized access, OTP was obligated to act with reasonable care to protect against these foreseeable threats.

65. OTP's duty also arose from OTP's position as a business associate. OTP holds itself out as a trusted business associate of healthcare providers, and thereby assumes a duty to reasonably protect the information it obtains from its Customer-Healthcare Providers. Indeed, OTP, which receives, maintains, and handles PII and PHI from its Customer-Healthcare Providers, was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

66. OTP breached the duties owed to Plaintiff and Class Members and thus was negligent. Although the exact methodologies employed by the unauthorized third parties are

unknown to Plaintiff at this time, on information and belief, OTP breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

67. But for OTP's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised.

68. As a direct and proximate result of OTP's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to OTP with the mutual understanding that OTP would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in OTP's possession and is subject to further breaches so long as OTP fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

69. As a direct and proximate result of OTP's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(ON BEHALF OF PLAINTIFF AND THE CLASS)

70. Plaintiff restates and realleges all proceeding factual allegations above as if fully set forth herein.

71. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as OTP or failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of OTP's duty.

72. OTP violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. OTP's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored and the foreseeable consequences of a data breach involving patient PII and PHI obtained from its Customer-Healthcare Providers.

73. OTP's violation of Section 5 of the FTC Act constitutes negligence *per se*.

74. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

75. OTP is an entity covered under the HIPAA, which sets minimum federal standards for privacy and security of PHI.

76. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et. seq.*, and its implementing regulations, OTP had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiff's and the Class members' electronic PHI.

77. Specifically, HIPAA required OTP to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq*.

78. HIPAA also requires OTP to provide Plaintiff and the Class Members with notice of any breach of their individually identifiable PHI "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach." 45 CFR §§ 164.400-414.

79. OTP violated HIPAA by actively disclosing Plaintiff's and the Class Members' electronic PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI; and by failing to provide Plaintiff and Class members with notification of the Data Breach within 60 days after its discovery.

80. Plaintiff and the Class Members are patients within the class of persons HIPAA was intended to protect, as they are patients of OTP's Customer-Healthcare Providers.

81. OTP's violation of HIPAA constitutes negligence *per se*.

82. The harm that has occurred as a result of OTP's conduct is the type of harm that the FTC Act and HIPAA was intended to guard against.

83. As a direct and proximate result of OTP's negligence, Plaintiff's and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY / BREACH OF DUTY OF CONFIDENTIALITY
(ON BEHALF OF PLAINTIFF AND THE CLASS)

84. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

85. Plaintiff and Class Members have an interest, both equitable and legal, in the PII and PHI about them that was conveyed to, collected by, and maintained by OTP and that was ultimately accessed or compromised in the Data Breach.

86. As a business associate of its Customer-Healthcare Providers and recipient of patients' PII and PHI, OTP has a fiduciary relationship to its customers' patients, like Plaintiff and the Class Members, and it owes them, at a minimum, an implied duty of confidence and confidentiality.

87. Because of that fiduciary and special relationship and the nature of the sensitive data OTP received, when OTP was provided with and stored private and valuable PHI related to Plaintiff and the Class, Plaintiff and the Class were entitled to expect their information would remain confidential while in OTP's possession, even in the absence of direct privity between them.

88. OTP owed a fiduciary duty and a duty of confidence under common law to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

89. OTP breached the duties owed to Plaintiff and Class Members. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiff at this time, on information and belief, OTP breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

90. But for OTP's wrongful breach of its duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised.

91. As a direct and proximate result of OTP's breaches of its fiduciary duty and duty of confidentiality, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to OTP with the mutual understanding that OTP would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in OTP's possession and is subject to further breaches so long as OTP fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

92. As a direct and proximate result of OTP's breach of its fiduciary duty, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFF AND THE CLASS)

93. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

94. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

95. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether OTP is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that OTP's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his PII and PHI and remains at imminent risk that further compromises of his PII and/or PHI will occur in the future.

96. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. OTP owes a legal duty to secure patient PII and PHI obtained from its Customer-Healthcare Providers and to timely notify such patients of a data breach under the common law, Section 5 of the FTC Act and HIPAA.

b. OTP breached and continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI.

97. This Court also should issue corresponding prospective injunctive relief requiring OTP to employ adequate security protocols consistent with law and industry standards to protect patients' PII and PHI.

98. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at OTP. The risk of another such breach is real, immediate, and substantial. If another breach at OTP occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

99. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to OTP if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to OTP of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and OTP has a pre-existing legal obligation to employ such measures.

100. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at OTP, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all other similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: August 9, 2022

Respectfully Submitted,

/s/ Gary F. Lynch

Gary F. Lynch
Nicholas A. Colella*
Hannah Barnett*
LYNCH CARPENTER, LLP
1133 Penn Ave., Fl. 5
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
gary@lcllp.com
nickc@lcllp.com
hannah@lcllp.com

Counsel for Plaintiff

*Petition for admission to be filed.